



AI Responsible Use Policy

Effective March 2025

INTRODUCTION

Artificial Intelligence (**AI**) is becoming increasingly prevalent across a broad range of industries, such as legal, finance, bio-science industries, as well as our individual day to day lives. With the appropriate protocols, AI can help us to perform a variety of tasks more efficiently within a fraction of the time that it would take to complete manually. When DFIN develops AI Systems it should be thoughtful in its design

This policy outlines the risks of using of AI at Donnelley Financial Solutions, Inc. (**Company** or **DFIN**) especially pertaining to the of use of confidential Company or client data.

Purpose

The purpose of this AI Responsible Use Policy (**Policy**) is to establish guidelines on how to safely and lawfully use and develop AI Systems at DFIN.

Scope

Every global DFIN employee is expected to understand and follow this Policy. This Policy also applies to contractors, consultants, and other parties who have access to DFIN's data and AI Systems or play a role in their development. The term "**Personnel**" as defined below is used throughout the Policy to describe the scope of covered individuals.

Nothing in this Policy is intended to nor shall modify or supersede any of DFIN's other policies and procedures that Personnel are subject to, nor does this Policy limit our efforts to comply with any applicable law or regulation and other governance documents. Nothing in this Policy is intended to violate any local, state, federal, or international law.

Definitions

AI Model: A program that uses algorithms and data to learn patterns and make decisions with limited human intervention. One or more AI Models may be integrated into and used to operate an AI System.

AI Oversight Committee: DFIN's designated leaders responsible for overseeing the Company's responsible and lawful use and development of AI Systems. This committee is comprised of a cross-functional group of leaders who will interpret this Policy, review and address reported concerns about DFIN's use and development of AI Systems, and provide direction, support, and training so that this Policy can be effectively implemented.

AI Provider: A processor, service provider, contractor, vendor or other similar terms that represent a natural or legal person, public authority, agency or other body that processes Personal Information on DFIN's behalf or to whom we make Personal Information available. An AI Provider also includes within its scope any external third party that provides support to DFIN for AI use and development.

AI System: Any machine learning, deep learning, or other artificial intelligence technologies, including statistical learning algorithms, models (including large language models), neural networks, and other artificial intelligence tools or methodologies, and any software implementations of any of the foregoing, capable of generating various types of content (including



text, images, video, audio, or computer code, decisions, analysis, predictions or recommendations) based on user-supplied prompts.

Algorithmic Discrimination: Any condition in which the use of an AI System results in unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of their actual or perceived age, color, disability, ethnicity, genetic information, limited proficiency in the English language, national origin, race, religion, reproductive health, sex, veteran status, or other classification protected under applicable state or federal laws.

Confidential Information: Information that pertains to (a) know-how, trade secrets, tools, constructions, methods, methodologies, techniques, designs, specifications, projections, computer source code, customer lists, pricing information, marketing plans, personnel information, financial information, and business strategies, (b) other information that, a reasonable person would conclude, is intended to remain confidential, due to its nature or the circumstances under which it is disclosed, (c) any other non-public information that DFIN designates orally or in writing as confidential.

Individual Data Subject: A natural person or consumer who receives rights and protections under data protection or AI laws.

Personal Information: Any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with an individual. Personal Information also includes information referred to as “nonpublic personal information,” “personally identifiable information (PII)” or “personal data (PD)” under data protection laws.

Personnel: All Company officers employees, consultants, and contractors, as well as AI Providers and other parties who have access to DFIN's Confidential Information and AI Systems and/or play a role in the development of AI Systems.

Sensitive Personal Information: This includes, but is not limited to an individual's: (a) social security, driver's license, state identification card, or passport number; (b) account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account; (c) citizenship or immigration status; (d) precise geolocation; (e) racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; (f) mail, email, and text messages contents, unless DFIN is the intended recipient of the communication; (g) genetic data; (h) mental or physical health diagnosis or other health data; (i) biometric data; (j) sex life or sexual orientation and status as transgender or non-binary; (k) status as a victim of crime; (l) criminal convictions and offences; (m) financial information, (n) neural data, and any (o) Personal Information of a child.

Serious Incident: An incident involving an AI System that requires notification and/or reporting under AI laws, including, as applicable, any incident that directly or indirectly leads, might have led or might lead to (a) Algorithmic Discrimination, (b) a serious and irreversible disruption of the management and operation of critical infrastructure; or (c) the death of a person or serious damage to a person's health, property, or to the environment.

Principles for Safe, Secure and Trustworthy AI

When DFIN develops or uses AI Systems, we are committed to adhering to the following principles, which align with DFIN's ethical values and are intended to mitigate AI risks and ensure

that we utilize such technology in a safe, secure, and trustworthy manner. We recognize that AI Systems vary and present different risks to DFIN's information and stakeholders based on the intended use. Prior to using any AI System, Personnel shall review specific instructions, training, guidelines and other information provided by DFIN (or the vendor, as applicable) for that tool, as that documentation will further define these principles for the applicable context.

- **Transparency and Explainability.** AI Systems should be used in a manner that is transparent and explainable. Personnel are accountable for the uses and impacts of AI Systems and should be transparent with relevant stakeholders about how we use AI Systems and their outcomes. For AI Systems developed by DFIN, this includes providing clear information about the training, capabilities, limitations, and potential effects of the AI Systems. For AI Systems developed by a third party but used by DFIN, this includes understanding intended use cases and providing clear guidance about the training, capabilities, limitations, and potential effects of the AI Systems. Personnel must also disclose and label AI-generated material as such and ensure that the use of AI Systems in creating content is transparent to others, even if only for idea generation. Depending on applicable law, DFIN may need to publicly post on its website our use and development of AI Systems to demonstrate transparency and explainability.
- **Safety.** DFIN's AI Systems must be designed, built, and operated with a primary focus on safety and quality principles. Careful consideration should be given to all AI Systems intended and unintended uses or impacts, and protective measures (such as instructions, pre-deployment testing, risk identification and mitigation). Personnel should be aware of the potential misuse of AI which could result in cyberthreats, deepfakes (which can be used to deceive), and the spread of inaccurate or biased information. Ongoing monitoring should be undertaken to mitigate unsafe outcomes. Personnel should use good judgment when using AI Systems to protect themselves and other stakeholders.
- **Accuracy, Robustness, and Reliability.** AI Systems must be used as a tool and resource to assist Personnel, not as a replacement for human judgment and expertise. Personnel must take reasonable steps to determine the accuracy, robustness, and reliability of any AI System and its outputs. Personnel must ensure that the AI System (or AI Model that is being trained or fine-tuned) is operating as intended and avoids unexpected or surprising results, including by performing regular testing on datasets, measuring the performance of the system under a variety of circumstances, and conducting ongoing monitoring. Since reliability of AI Systems is unclear, do not assume accuracy or completeness in AI outputs even if using AI Systems for authorized uses and in compliance with our policies and guidelines. A second source should also be used, where available, to verify the accuracy of output of AI Systems. Appropriate human interaction and oversight should be built into AI Systems to ensure accuracy, completeness, and protection of both third-party rights and our Confidential Information. Personnel are ultimately responsible for all content produced with the assistance of AI Systems, as if they were the original creators.
- **Intellectual Property (IP) Rights.** Personnel must ensure that AI Systems are used in a manner that respects the IP rights of DFIN and of third parties. Careful consideration should be given to any applicable restrictions on the use of third-party training data as well as whether the output of AI Systems violates any third-party or individual's rights. Human involvement should be documented to identify human contributions to any IP that arise from the implementation of AI Systems so that DFIN may take steps to protect its own work under applicable IP laws.

- **Ethical, Fair, and Non-Discriminatory.** Personnel must take reasonable steps to ensure that AI Models are trained, and AI Systems are used in a manner that is ethical, fair, and avoids harmful bias and Algorithmic Discrimination. Data inputs should be proactively assessed to minimize unintentional bias and ensure the use of data that is representative of the population it is meant to reflect. AI outputs should be regularly monitored for unintended and unjustified consequences, harms, and disparate impacts. Where Sensitive Personal Information is involved, please contact the AI Oversight Committee to determine appropriate data scientists, engineers, lawyers, and other professionals to advise on whether the AI System is developed and used pursuant to industry best practices and relevant legal standards.
- **Secure.** Personnel must employ and ensure adequate security mechanisms and protections are in place for AI Systems to maintain their availability, confidentiality, and integrity. Personnel must also ensure that AI Systems are not used in a manner that risks the safety, security, and trustworthiness of DFIN's non-AI Systems. DFIN maintains a rigorous Information Security Program that safeguards our information assets against unauthorized use, disclosure, modification, damage, or loss. AI Systems may only be used and developed in accordance with DFIN's information security policies and procedures.
- **Compliant with Information Security and Data Privacy Requirements** such as:
 - **Legitimate Purpose.** The legitimate purpose of any use of Personal Information in AI Systems should be identified clearly, and AI Systems should not be used for any purpose that does not align with DFIN's mission and values.
 - **Purpose Limitation.** Personnel may only use Personal Information in AI Systems for the explicit, legitimate, and express purposes specified in an appropriate privacy notice. Personal Information should not be further processed in AI Systems if it is incompatible with those purposes. If Personnel plan on using Personal Information in an AI System for reasons other than as described in the relevant privacy notice, an individual's consent may need to be obtained, or relevant contractual terms agreed, depending on applicable data protection laws.
 - **Data Minimization.** Personnel should take all reasonable steps necessary to limit using Personal Information in AI processing. Only Personal Information that is adequate, relevant, and limited to what is reasonably necessary for the AI processing should be considered for usage within an AI System. As appropriate, pseudonymized, de-identified, aggregated, anonymized, and synthetic data should be used instead of Personal Information.
 - **Storage Limitation.** Personnel must ensure that any Personal Information used as input data for AI processing or that is revealed in the output data, is retained only as long as necessary for the purposes for which the Personal Information was processed.
- **Prohibition on Disclosure of Confidential Information.** Personnel are prohibited from using Confidential Information in AI processing unless they provide notice to and obtain approval from our AI Oversight Committee. Personnel should treat all information provided to an AI Model or AI System as if they were posting it on a public site or social platform. If in doubt about whether information should be treated as Confidential Information, refer to [DFIN's Information Classification Standard and Procedure](#) for additional guidance. Personnel should err on the side of not uploading, sharing, or providing information into an AI System prior to properly classifying the data type.

- **Accountability.** Personnel are accountable for the proper functioning of AI Systems consistent with the above principles, based on their roles, the context, and the state of the art of the AI System. If you are unsure whether a particular situation or activity amounts to a violation of law or a violation of this Policy, please contact your supervisor or manager, the Chief Compliance Officer or other a member of the AI Oversight Committee before doing anything.

AI Features in Third-Party Products

Identifying Use of AI in Existing Systems

In order to sustain DFIN's security best practices, we must evaluate the AI capabilities for any third-party product or service so that we can appropriately assess and manage any security threats and other risks. This requires Personnel to exercise due diligence to help identify when existing tools and products used at DFIN have evolved to include AI advancements.

Stay alert for the following updates and notices related to potential AI advancements within third party products:

- Marketing materials for new versions of their products.
- Vendor announcements and blogs.
- Tooltips or captive popups that inform users of new features or suggest shortcuts.
- Documentation and release notes.
- New terms and conditions which include AI related provisions.
- Community forums and user groups.

Personnel may receive clues that a product incorporates AI if the product/tool supports the following list of popular commercial and Open Source AI libraries/APIs in use today, such as: OpenAI/ChatGPT, PyTorch, TensorFlow, Hugging Face, IBM Watson, Microsoft Cognitive Toolkit (CNTK), Scikit-Learn, Keras, LangChain, Deeplearning for Java(DL4J).

If any new or existing tools are incorporating AI into their product or service, please contact DFIN's Procurement team to launch a review by DFIN's Privacy, Security, and Governance teams.

Evaluating and Documenting Use of AI Systems

Personnel are required to inform their supervisor or manager and the Procurement team if they believe that an existing/approved tool or product has been developed to include AI functionality or if they are considering a new vendor or product that incorporates AI functionality. All products and tool advancements leveraging AI functionality must be assessed through the appropriate security management channels at DFIN. DFIN's Privacy, Security, and Governance teams must evaluate these products and tools for any threats before these AI Systems may be authorized for use within DFIN. All AI Systems that incorporate Personal Information in the input of the training data need to be reviewed and approved by DFIN's Privacy, Security, and Governance teams before usage. Such AI Systems will be vetted to understand whether and how Personal Information is being used and retained and what controls are in place to protect the Personal Information among other topics. Personnel are also responsible for working with DFIN's Privacy team to ensure that their use and development of AI Systems is documented in DFIN's IT asset and data inventory and that DFIN has a record of the AI System's input or training data, where



information for the training data came from, how it was collected, curated, and moved within the Company.

We will continue to raise questions and initiate discussions with our vendors regarding the security parameters and features of any AI developments with our third-party products/tools. These considerations include but are not limited to:

- **Business Justification** – Evaluation of the benefits of introducing the AI system or any associated developments to DFIN while undergoing security management of any potential risks before implementation within the business processes.
- **Vendor/Product Research** – Consideration of the reputation, history, and any previous security violations associated with the vendor and if there are any third-party concerns.
- **Data Privacy / Security Considerations** – Consideration pertaining to how the product handles data inputs. Does it retain data for learning?
- **Associated Third Party Considerations** – Investigation of any third-party associated applications or services in collaboration with the product/tool.
- **AI Model Transparency** – Evaluation of the transparency on model training data, biases within outputs, and explainability for accuracy of results.

Personnel that transfer Personal Information or make it available to an AI Provider or otherwise utilize AI Processors in connection with the use or development of AI Systems, are required to coordinate with DFIN's Procurement team to enter into an appropriate agreement with the AI Provider in compliance with applicable laws and commercial best practices. DFIN's Legal Department can assist with ensuring that vendor agreements comply with DFIN's standard terms and applicable laws.

Acceptable Uses for AI Systems at DFIN

Below is a list of acceptable use cases for AI Systems within DFIN. With the implementation of any AI System, Personnel must continue to adhere to the security and data protection guidelines set out within the [DFIN Information Classification Standard and Procedure](#) and comply with other instructions or parameters specific to your use case.

- **Editing:** Including creating a draft output of text in desired format or tone, summarizing text.
- **Research:** Locating answers to input based on non-Confidential prompts or data or offering shortened versions of public articles, emails, or webpages.
- **Classification of content:** Automated arrangement of topics, commonalities, etc.
- **Customer support and performance improvement:** Generating journey flows from general descriptions input, sentiment classifications, and extractions.
- **Software coding:** Code generation, optimization, translation, explanation, review, and verification.

Annex A includes a list of the AI Systems currently approved for staff use at DFIN. These tools have been carefully assessed for relative security risks and the list will be updated regularly. Please refer to the intranet for information about accessing these tools and for specific guidelines, instructions and approved use cases.

In order to maintain the enhanced security safeguards at DFIN, we urge all Personnel to follow these AI usage guidelines:

1. **Don't** use unapproved AI Systems (e.g. ChatGPT, Gemini) and **Don't** use approved AI Systems in a manner that is not permitted under the instructions for use or terms agreed.
2. **Don't** input any customer data, Personal Information or Sensitive Personal Information into the AI System unless the AI System has been approved for that use case.
3. **Don't** input any DFIN IP or use an AI System to gain information that may be the IP of third parties.
4. **Don't** use personal accounts with AI Systems for Company-related purposes.
5. **Do** disable history if using external tools that enable that choice.
6. **Do** closely evaluate outputs. These are sometimes subject to subtle (but meaningful) AI hallucinations, factual errors, and biased or inappropriate statements.
7. **Do** submit third party tools for review when AI features are discovered, enabled, or made available.
8. **Do** work with your manager or supervisor to have new AI solutions approved for DFIN use to increase productivity.

Prohibited Uses for AI Systems at DFIN

Laws and regulations governing AI Systems are rapidly evolving. The AI Oversight Committee will conduct periodic assessments to ensure that the use of AI Systems is compliant and lawful. Personnel should be aware of compliance requirements when developing or using AI Systems. This includes laws and regulations that are not specific to an AI System but apply based on how it is used.

Certain AI Systems are prohibited under applicable laws. These include, but are not limited to AI Systems that:

- Use subliminal techniques to distort a person's behavior in a harmful manner.
- Are used to exploit vulnerabilities of disadvantaged groups (e.g., due to age, disability, social or economic situation, and other protected classifications).
- Use Personal Information of children under 18 years of age as an input or to train an AI Model.
- Are used for social scoring based on social behavior or personal characteristics.
- Are used to create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage.
- Are used for emotion recognition in the workplace.
- Are used for biometric categorization to infer certain Sensitive Personal Information.
- Are used for predictive discipline.
- Discriminate against an applicant or employee due to protected classifications.
- Create unfair and deceptive practices.
- Cause Algorithmic Discrimination.

High Risk Uses of AI Systems

As part of DFIN's risk management activities and as required by applicable law, Personnel must consult with the AI Oversight Committee to conduct an AI assessment when engaging in high-risk AI. The AI assessment will document and rank the AI risks, assess the likelihood and severity of AI harms, and describe the mitigation measures implemented to reduce risks. AI assessments are a continuous and iterative process that should run throughout the entire lifecycle of the AI System. Personnel that believe an AI System is high-risk should notify the AI Oversight Committee.

Examples of high-risk AI include, but are not limited to, AI Systems in connection with:

1. Processing Sensitive Personal Information.
2. Biometric identification and surveillance.
3. Human resources functions (employment decisions, including recruitment, hiring, allocation or assignment of work, compensation, retention, promotion, transfer, performance monitoring, demotion, suspension, dismissal, and referral).
4. Education and vocational training.
5. Intrusion upon solitude, seclusion or private affairs of individuals.
6. Extensive profiling, such as: (a) systematic observation of individuals when they are acting in their capacity as an applicant to an educational program, job applicant, student, employee, or independent contractor; (b) systematic observation of a publicly accessible place; or (c) behavioral advertising.
7. Selling or sharing Personal Information.
8. Processing Personal Information to train AI Systems.
9. Activities that can cause other legal or other significant impact on individuals.

Data Deletion Requests

Under data protection and AI laws, Individual Data Subjects have certain rights, such as the right to access, delete, correct, and to opt out of certain processing activities and decisions made with AI Systems. AI Systems must implement appropriate policies and procedures to process Individual Data Subject's requests. If Personnel receive a deletion request from an Individual Data Subject, direct the request to dataprivacy-internal@dfinsolutions.com. DFIN's Privacy team will handle the request and submit it through DFIN's designated methods for processing.

Monitoring and Reporting

Compliance and Oversight

This Policy will be reviewed by the AI Oversight Committee and updated in line with relevant AI, data privacy, and compliance legislation as necessary in order to ensure that it remains current and effective. The latest version of this Policy can be found on DFIN's Intranet. Periodically, DFIN will hold training sessions for Personnel to learn how to use and develop AI Systems in compliance with applicable laws and regulations, in accordance with DFIN's policies, procedures, guidelines, and developments in AI technology. All Personnel are obligated to complete any assigned training and act in accordance with that training.

DFIN has monitoring procedures designed to detect violations of this Policy. However, if you become aware of an ethical or legal violation, including violation of this policy or any other DFIN policy, you have an obligation to report it to the Company as described below.

The AI Oversight Committee must approve any waiver of this policy, in writing. Waivers of this policy may also require approval of the Board of Directors (or a designated committee) and will be disclosed to the extent required by applicable law or regulation.

Incident Reporting

DFIN's Information Technology (IT) systems are fundamental to business operations, and any problem affecting corporate environment IT resources can quickly impact the business. Responding efficiently and effectively to security incidents is crucial for minimizing risks to the business, customers, and other stakeholders. If you have reason to believe that your or another person's use or development of an AI System may have been subject to a data security incident



or Serious Incident, please contact the Cyber Security Incident Response Team at security@dfinsolutions.com. For any AI System incident involving Personal Information, DFIN's Privacy team should also be immediately contacted at dataprivacy-internal@dfinsolutions.com.

Violations of this Policy

Personnel that become aware of a violation of law or this Policy, should immediately report this information to their supervisor, manager, the Chief Compliance Officer, or a member of the Legal Department. Alternatively, if you wish to remain anonymous, you may report your concerns using the Company's Ethics Reporting platform via web application, text or online at mobile.reportit.com using the code "DFIN". Additional details, links, and QR Codes to access the Ethics Reporting platform can be found on the Company's intranet.

When reporting a violation or incident, be sure to provide enough information for the Company to be able to follow up (for example, names of persons allegedly involved, dates and nature of activity). The Company will investigate all reports of violations. Do not investigate the matter on your own, rather leave such work to the designated people chosen by the Company.

No Personnel should make a false report of a violation. No Personnel will be penalized for making a good-faith report, nor will the company tolerate retaliation against an employee who makes a good-faith report.

If you report a violation and are in some manner also involved in the violation, the fact that you stepped forward will be taken into consideration. Nothing in this Policy shall be construed to prevent disclosure of Confidential Information as may be required by applicable law or regulation. In addition, this Policy is not intended to and shall not be enforced in such a way as to prevent Personnel from exercising any rights they may have under applicable employment, privacy, or whistleblower laws.

While reports of violations should be addressed to your supervisor, management, or the DFIN Ethics Reporting platform, questions regarding laws or the Company's policies may be directed to the Chief Compliance Officer.

Questions and Contact Information

If Personnel have any questions regarding their use or development of AI Systems and this Policy, particularly AI practices that may constitute a prohibited or high-risk AI processing activity, they should contact the AI Oversight Committee at dataprivacy-internal@dfinsolutions.com.

APPENDIX

Other terms used in discussion of AI are defined below for greater context and clarity. Articles, white papers and other resources are available on DFIN's intranet for people who are interested.

AI Deployer: An individual, entity, public authority, agency, or other body that uses an AI System under its authority except where the AI system is used in the course of a personal non-professional activity.

AI Input: Any data, submission, prompt or other input that is submitted to or through an AI System to generate an output.

AI Output: Any data or other output that is generated or returned through the AI System.

Generative AI: A variant of AI that generates individualistic content in response to a user's request. Generative AI can be trained. The trained AI Models learn the patterns and configuration of their input in order to generate new data with comparable characteristics. Depending on said request, the output may be delivered in the form of text, audio, visuals, or other data. GenAI includes Generative Adversarial Networks (GANs), Transformers, and Large Language Models (LLMs), that have expanded its use and popularity today.

Large Language Model (LLM): A form of AI that utilizes deep learning algorithms to create models pretrained on massive text datasets for the general purpose of analysing and learning patterns and relationships among characters, words and phrases to perform text-based tasks. There are generally two types of LLMs: generative models that make text predictions based on the probabilities of word sequences learned from its training data and discriminative models that make classification predictions based on probabilities of data features and weights learned from its training data.

Narrow AI: AI usage that is limited in scope. These AI models are designed to perform very specific tasks or closely related tasks. Unlike Generative AI, Narrow AI is not adaptable or capable of replicating human intelligence. Narrow AI is one of the most common forms of AI in circulation today. This variant of AI is used on most smartphones with facial recognition or language translation apps such as Google Translate.

Annex A

March 3, 2025

The list below details AI technology that is provisionally approved for use at DFIN. As DFIN's IT governance, security and privacy teams continue to review tools and solutions, additional items will be added to the list and some may be removed. If you become aware of AI technology in use at DFIN that is not on this list, please contact security@dfinsolutions.com.

DFIN AI Technology (GenAI, NLP, ML)

- Microsoft CoPilot (basic version is approved, Copilot 365 is still in evaluation)

DFIN Tools and Solutions Leveraging AI Technologies

- Anomoli
- Darktrace
- Hypercomply
- MDE
- Microsoft DLP and IRM
- Microsoft O365/Teams
- Palo Alto NGFW
- Panorays
- Qualys VMDR and DAST
- Radware Cloud WAF/DDoS
- Reliaquest Grey Matter

Suppliers Leveraging AI Technologies Supporting DFIN (acknowledged as a part of SCS vetting)

- Accenture
- Algolia
- Applitools
- Asana AI
- Cohere
- Crossbeam
- DATEV eG
- Drift
- Elly
- Global Vision

- Gong
- Google Workspace
- Harness.io
- Heap
- Highspot
- HyperComply
- LearnExperts
- Microsoft Azure
- Panorays
- SAI360
- SDL Inc
- Skilljar
- Theloops
- TransPerfect
- WALKME, INC.
- Zywave